PATNA WOMEN'S COLLEGE 1940

Master of Computer Applications (MCA)

Explore–Journal of Research
ISSN 2278 – 0297 **(Print)**
ISSN 2278 – 6414 **(Online)**

http://www.patnawomenscollege.in/journal

Denial of Service Attack: Challenges faced by Internet Service Providers (ISPs)

• **Nishu Kumari** • **Ankita** • **Nimmi**
• **Samta Sinha**

Received : November 2016
Accepted : March 2017
Corresponding Author : Samta Sinha

Abstract : *Disruption of service caused by DDoS attacks is a serious threat to Internet today. These attacks can disrupt the availability of Internet services completely, by eating either computational or communication resources or graceful degradation of network performance. In this paper we have described the major services of Internet Service Providers which are under the threat of Denial of Service (DoS) attack and major challenges faced by ISPs due to it. We have also described the various types of DoS attack techniques that are inflicted upon the ISPs, their effect on business and limitations of measures taken by them to mitigate it. Finally, on the basis of our analysis we have tried to find possible solutions to overcome this major and hazardous attack on ISP.*

Keywords: *DoS, DDoS, ISP, attack.*

Nishu Kumari
MCA-Vth Semester, Session: 2014-2017,
Patna Women's College, Patna University, Patna,
Bihar, India

Ankita
MCA-Vth Semester, Session: 2014-2017,
Patna Women's College, Patna University, Patna,
Bihar, India

Nimmi
MCA-Vth Semester, Session: 2014-2017,
Patna Women's College, Patna University, Patna,
Bihar, India

Samta Sinha
Asst. Professor, Asst. Coordinator, Department of MCA,
Patna Women's College, Bailey Road,
Patna – 800 001, Bihar, India
E-mail : samta1sinha@gmail.com

Introduction :

The Internet is a part of the critical national infrastructure and is provided by the ISP. It is unique as it has no customary borders to safeguard it from attacks. One such attack is the DDoS .The number of DoS and DDoS attacks on the Internet Service Providers has risen sharply in the last several years. The advent of remote controlled networks of computers used to launch attacks has changed the landscape and methods that a service provider must use. Service providers are under mounting pressure to prevent, monitor and mitigate DDoS attacks directed toward their customers and their infrastructure.

Internet Service Provider (ISP) : An ISP is an organization that provides services for accessing and using the Internet. Internet service providers may be

organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Services provided by an ISP include Internet Access, Internet Transit, Domain Name Registration, Web Hosting, USENET Service, Co-location etc.

DDoS: A Major Threat to the ISPs : The impact of a successful DDoS attack on an ISP is widespread. Site performance is severely compromised, resulting in frustrated customers and other users. Service-level agreements (SLAs) are violated triggering off costly service credits. The growing dependence on the Internet makes the impact of successful DDoS attacks financial and otherwise increasingly painful for service providers.

DDoS on ISPs results in the following:-

- Lost revenue
- Lost productivity
- Increased IT expenses
- Mitigation costs
- Loss of customers

Understanding the DDos Attack : The Internet consists of hundreds of millions of computers distributed all around the world. The interconnectivity among computers on which the World Wide Web relies, renders it an easy target for launching Denial-of-Service (DoS) attacks. A Denial-of-Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet. According to B. B. Gupta et al (2008) CERT defines the term "Denial of Service" as "Occupancy of limited resource or difficult to renew resources such as network bandwidth, data structure or memory of a system". When many hosts coordinate to flood the victim with an abundance of attack packets, and the attack takes place simultaneously from multiple points it is called a Distributed DoS (DDoS) attack. In another form of DoS attack known as DRDoS (Distributed Reflector DDoS) it attacks the army of the attacker which consists of master zombies, slave zombies, and reflectors. A DRDoS attack is more detrimental than a typical DDoS attack.

Types of DDoS Attack

- **Flooding:** Available bandwidth is one of the "goods" that attackers try to consume by flooding the network with useless packets.
- **Protocol Violation Attacks:** The attacker is sending packets in a manner not originally intended.
- **CPU Power and Service:** By generating several thousands of useless processes on the victim's system, attackers manage to fully occupy memory and process tables. In this way, the victim's computer breaks down. Attackers can try to occupy victims' services so that no one else can access them.

Alternate attacks methods & their impact:

The major DDoS attacks on ISP network is the Network Infrastructure attacks. These have a serious impact on the overall operation of the ISP. These attacks can create regional or global network outages. These include:-

- **Control Plane Attacks**: Attackers direct DDoS attacks against the routing protocols and lead to regional outages. Attacks are usually directed at dynamic routing protocols such as BGP, OSPF etc.
- **Management Plane Attacks**: The management plane allows network operators the ability to configure the network elements. Attacks on management plane involve protocols such as telnet, SSH, HTTP, SNMP, NTP etc.
- **Network Services Attacks**: It aims at disrupting the basic services provided by and needed by the ISP. DNS is a critical network service for operation of the ISP as well as a service provided by the ISP. As a public service, DNS in a service provider's environment is the most targeted service.

Defence Challenges: Despite the tremendous efforts by researchers and experts to address the denial of service, it still remains an unsolved problem. The various technical and non-technical challenges underlying the inability to mitigate these attacks include:

1. Internet Architecture Related Challenges

- **On-demand resource sharing:** Inter-user dependency is a fundamental factor that enables denial of service to occur.

The fundamental structure of the Internet allocates link use on demand, and link capacity will be shared among the users. In such environment, a misbehaving user can disrupt service for other users by occupying most of the shared resources.

- **Decentralized management:** Current Internet can be seen as interconnection of many Autonomous Systems (AS). Each AS has its own set of operating policy and security policy. The enforcement of a global security policy or mechanism is enormously difficult, which makes solutions that require cross-domain cooperation unattractive.
- **Accountability:** Accountability ensures that the actions of an entity may be uniquely traced back to that entity. The indifference to accountability issue is now difficult to ignore.
- **Variation in link capacity:** The provisioning of link bandwidth in modern Internet varies significantly from core networks to edge networks (Bush and Meyer 2002). Traffic from the high-bandwidth core link can overwhelm the low-bandwidth edge link.

2. **Miscellaneous**
   - **Difficulty of distinguishing malicious requests:** It is difficult to distinguish between malicious requests and legitimate ones.
   - **Asymmetry of request and response overhead:** Asymmetry of request and response overhead refers to the asymmetry in the amount of consumed resources for generating a request at the client and creating response at the server. In most cases, a client spends a trivial amount of CPU and memory resources to generate requests, and the operations carried out by the server to produce the corresponding response incurs significantly more resource overhead in comparison.
   - **Research challenges:** Very limited information about DoS incidents are publicly available due to organizations' unwillingness to disclose the occurrence of an attack, for fear of damaging the business reputation of the victim. It becomes very difficult to compare the performance of various solutions. Moreover, the testing of DoS solutions in a realistic environment is immensely challenging, due to the lack of large-scale test beds or detailed and realistic simulation tools.
   - **Lack of core competency**: ISP's are in the business of selling bandwidth and don't always invest in the required capital and resources to stay ahead of the latest DDoS threats. According to some ISPs lack of ROI (Return of Investments) is a major discouraging factor.

Defence Mechanisms Used by ISPs:

- **Ingress/Egress Filtering:** The purpose of ingress/egress filtering is to allow traffic to enter or leave the network only if its source addresses are within the expected IP address range.
- Drawback: It is difficult to deploy ingress /egress filtering universally. If the attacker carefully chooses a network without ingress/egress filtering to launch spoofed DDoS attack, the attack can go undetected. Hence ingress/egress filtering are ineffective to stop DDoS attack. The possibility of multi-path routing diminishes routers' ability to determine spoofed source, since a router may receive an unexpected packet due to route changes (Clark 1988).
- **Black Holing:** ISP's use RTBH (remotely triggered blackholing), by which they can ask their upstream networks to discard the traffic, so it won't even reach the destination network.

  Drawback: The biggest target IP address (and thus the services running on it) is put offline exactly as the attackers want.

- **Monitoring:** Developed by Cisco, monitoring traffic patterns on DDoS attacks is a very popular tool used by ISPs. A flow is defined as having some unique attributes like source IP, Destination IP, Source port, Destination port etc. To monitor traffic in both directions all router interfaces must be monitored, including uplinks to the core routers.
- **Scrubbing:** The scrubbing centre has equipment to filter unwanted traffic, leaving a stream of clean traffic which gets routed back to the ISP.

  Drawback: Most scrubbing centres are commercial, and can cost quite a lot. Also, scrubbing is not always easy.

Objectives :

- Assess and classify the various types of threats DoS inflicts on ISPs (local and tier-3).
- Assess and classify the measures taken by ISPs against DoS attack.
- Assess the drawback of their measures to defend against DoS attack.
- Try to devise a better solution to defend ISPs against DoS attack.

Methodology :

- **Area of Study :** Survey of Physical Offices of Local ISPs and Tier-3 ISPs and websites.
- **Tools and Techniques for Data Collection**

  Questionnaire/Interviews

  Online Survey

  Document Analysis
- **Method(s) of Data Analysis :** We have compiled the total research work on the basis of two basic tools of MS-Office i.e., MS-Word and MS-Excel. Subsequently, we have modified the content of our research and findings in the form of a research paper and made a PowerPoint presentation using MS-PowerPoint.

Observations :

The impression drawn from this research study specifies and highlights the following facts:

1. Among the five major ISPs in India Bharti Airtel leads the market and holds 25.24 % of the market share as per graph in **Fig I**.
2. NTP Amplification DDoS attack showed an immense rise in the year 2014 and consisted of 33% of global DDoS attacks as per the graph in **Fig II**.
3. An exponential increase in all types of DDoS attacks was witnessed in the year 2015 as can be seen in **Fig III.**
4. Graph in **Fig IV** shows the major increase in source countries responsible for DDoS attacks in which China tops the list with 37.01%.
5. Data gathered in the third quarter of 2015 in **Fig V** shows that the gaming industry was the major target of DDoS attacks with flood rate 149 Gbps.
6. The Graph in the **Fig VI** shows that revenue wastage for preventing DDoS attacks has increased sharply at a rate of 25% and is expected to do the same by 2017
7. Both local and Tier III ISPs have set up a special security team and the number of team members in local ISP is around 8 while that of Regional ISPs is around 10 as shown by the graph in **Fig VII**
8. Local ISPs need around 4mins to detect attacks while the larger ISPs who witness more complex attacks need at least 10 minutes as per graph in **Fig VIII**.
9. Local ISPs use simple mechanisms of DDoS prevention like user login and traffic monitoring unlike Tier III ISPs which use logs based on server performance etc. as shown in **Table I.**
10. DDoS response techniques also vary as per the size of their businesses. Sophisticated techniques like IDS, IPS and deep packet inspection are used by

regional ISPs while local ISPs stick to simpler ones like firewalls as per **Table II**.

Major Finding :

1. DDoS attacks have become more sophisticated in the last several years.
2. ISPs are now increasingly targeted by DDoS attacks which are a hybrid of two or more DDoS attack types.
3. The solutions adapted by ISPs are proportionate to the size of their businesses.
4. Tier III ISPs have satisfactory resources and revenue to tackle DDoS but the local ISPs have to struggle to maintain a balance between their need for security and the profit in their business.

Solution and Method for Protecting Information:

Based on our findings we recommended some measures to local ISPs to strengthen security against DDoS attack in an economical manner. These include:

- Every single user who accesses your router should be given a username and password.
- Make sure you have RPF (ingress and egress filtering) on the interface of every static connection.
- Disable Telnet on vtys and allow only SSH based connections.
- Use Vtys filters to prevent public routers from getting response from your router.
- Use TACACS (Terminal Access Controller Access Control System) for password verification.
- Set up security labs. If not possible, set aside at least one spare router and server to try a new service instead of implementing it directly on the live network.
- Minimizing the number of transit providers, possibly one.
- Team up with other local ISPs for benefits like leasing a scrubbing centre, out of band management and possibly setting up better security labs.

Conclusion :

DDoS is becoming a major component of a long term threat campaign and the level of attack automation has escalated. Several efforts are being made by ISPs to combat it but they are still not able to overcome the problem completely. Instead, they are likely to pose a bigger danger in future. Several weaknesses, like the distributed and non-uniform architecture of the Internet infrastructure, business policies, privacy policies and return on investment has lowered the interest of ISPs in eradicating DDoS completely. Instead DDoS protection is itself growing as a new market. Under such circumstances, it seems impossible to completely eradicate DDoS from society. By following the recommendations given in the paper, local ISPs will be able to cope with DDoS attacks more effectively.

Future Scope : While all tiers of network providers are taking individual precautions, there is a need for unification of the efforts. The distributed nature of the DDoS attacks can be mitigated by a United effort where the local ISPs provide DDoS protection to Customers while Connection Providers (Transit Providers) make available DDoS protection to local ISPs. This hierarchical defence structure will cover security loopholes at all levels and will successfully give DDoSers a hard time.

LIST OF TABLES

Table I. Market share of five major ISPs in India

ISPs	Bharti Airtel	Vodafone	Relience Comm	Idea	BSNL	Other
Total Market Share (100)	25.24	21.09	11.20	11.06	10.59	20.82

Table II. Types of DDoS attack in 2014

Types of DDos attack	NTP Ampli-fication	Multi - Vector	TCP SYN fication	SSDP Ampli-	DNS Ampli-	Other
Total (100%)	33	15	16	10	6	20

Table III. Percentage of DDoS attack by month in 2015

	DNS Ampli-	SSDP Ampli-	Multi - Vector	TCP SYN	Other	NTP Ampli- fication
JAN	4	0	0	17	4	28
FEB	7	0	0	4	6	7
MAR	0	0	0	0	0	20
APR	0	0	18	32	0	8
MAY	12	0	34	20	10	18
JUNE	10	3	10	32	8	43
JUL	18	0	25	10	14	30
AUG	20	0	0	5	16	35
SEP	7	16	30	20	5	10
OCT	0	15	28	23	1	28
NOV	5	16	35	23	5	18
DEC	0	40	7	23	2	22

Table IV. Source countries for DDoS Attack

Coun- tries	China	US	UK	India	Spain	Korea	Russia	Germany	Australia	Taiwan
Total (100%)	37.01	17.88	10.21	7.43	6.03	4.53	4.45	4.29	4.18	4

Table V. DDoS attack more than 100 Gbps

Industry	Speed of DDoS attack in month of July	Speed of DDoS attack in the month of August
Media and Entertainment	146 Gbps	109 Gbps,145 Gbps
Financial Services	117 Gbps	106 Gbps
Gaming	149 Gbps	_
Software and Technology	_	127 Gbps, 134 Gbps

Table VI. Total revenue wastage on DDoS attack

Year	2012	2013	2014	2015	2016	2017
Total Revenue in Rupees	18301.25	22876.5665	27451.879	32027.1915	36602.504	41177.8165

Table VII. No. of team members

ISP	Local ISPs	Tier 3 ISP
No. of people involved	8	10

Table VIII. Time taken to decide

ISPs	Local ISPs	Tier 3ISPs
Time taken (in min.)	5	10

Table IX. Components for preventing DDoS

LOCAL ISP	TIER 3 ISPS
TRAFFIC CHEKING USER LOGIN	• LOGS • Servers performance- CPU, RAM • SOFTWARE UPGRADES

Table X: Parameters for Defeating DDoS attack

LOCAL ISP	TIER 1 ISPS
JUNIPERS FIREWALLS	• IDS • IPS • Web Application Firewall • DDOS mitigation tools • CLOUD based

LIST OF FIGURES

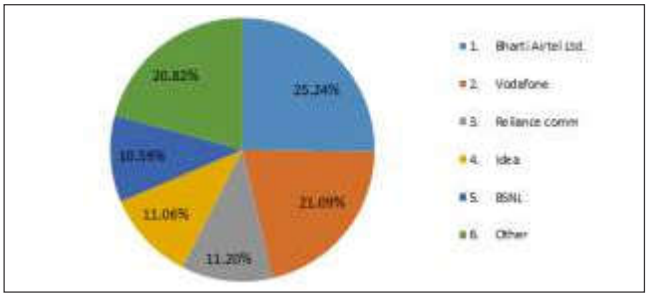

Fig. I. Market share of five major ISPs in India

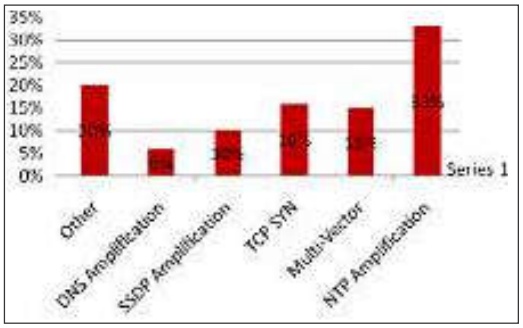

Fig. II. Types of DDoS attack in 2014

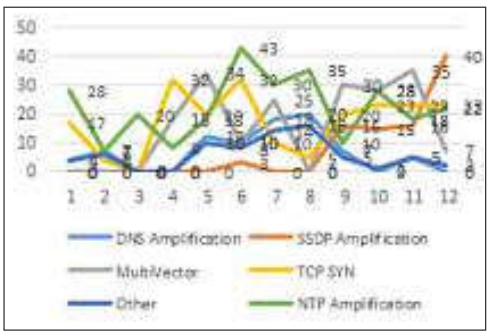

Fig. III. Percentage of DDoS attack by month in 2015

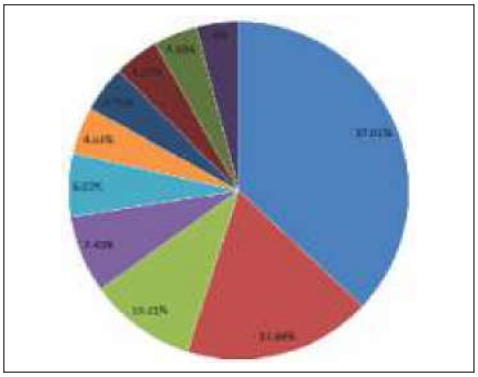

Fig. IV. Source countries for DDoS Attack

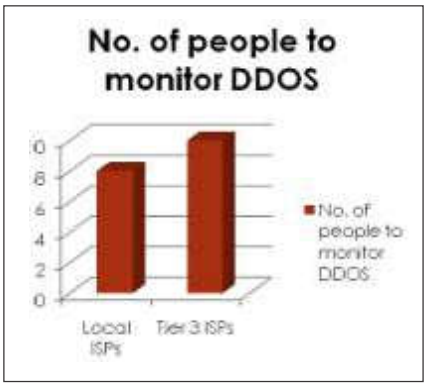

Fig. VII. No. of team members

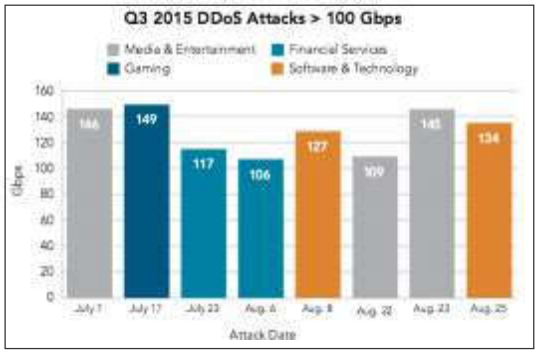

Fig. V. DDoS attack more than 100 Gbps

Fig. VIII. Time taken to decide

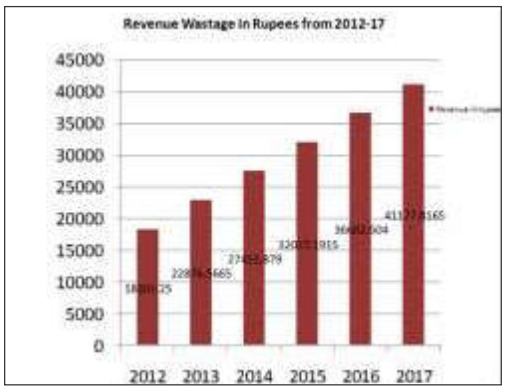

Fig.VI. Total revenue wastage on DDoS attack

References :

B. B. Gupta, Manoj Misra and R. C. Joshi (2008).'1 Journal of Information Assurance and Security 2 102-110 'An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach'

Srinivas Arukonda, Samta Sinha (2015). ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 1, No.13, ISSN : 2322-5157 www.ACSIJ.org, 'The Innocent Perpetrators: Reflectors and Reflection Attacks'